Calhoun: The NPS Institutional Archive

DSpace Repository

Center for Cybersecurity and Cyber Operations (C3O) Faculty and Researchers' Publications

2013

CyberCIEGE (brochure)

Naval Postgraduate School (U.S.); Center for Information Systems Studies Security and Research (CISR)

https://hdl.handle.net/10945/35361

This publication is a work of the U.S. Government as defined in Title 17, United States Code, Section 101. Copyright protection is not available for this work in the United States.

Downloaded from NPS Archive: Calhoun

http://www.nps.edu/library

Calhoun is the Naval Postgraduate School's public access digital repository for research materials and institutional publications created by the NPS community. Calhoun is named for Professor of Mathematics Guy K. Calhoun, NPS's first appointed -- and published -- scholarly author.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

Cyber CIEGE

Can you keep the network alive?

CyberCIEGE

CyberCIEGE enhances information assurance education and training through the use of computer gaming techniques such as those employed in well-known commercial resource management and simulation games. Player spend virtual money to operate and defend their networks, and can watch the consequences of their choices, while under attack.

Risk Management

In its interactive environment, CyberCIEGE covers the significant aspects of network management and defense. Users purchase and configure workstations, servers, operating systems, applications, and network devices.

The player makes trade-offs and prioritization decisions as they struggle to maintain the ideal balance between budget, productivity, and security. The player advances through a series of stages and must protect increasingly valuable corporate assets against escalating attacks.

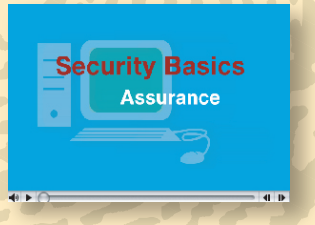
Game Characters

The behavior of the game's various virtual characters is defined by their goals. The following list enumerates the different character roles within the game.

- **Typical User** - Just wants to do the job. Dislikes hassles. Willing to learn new things (e.g., via training), but will find an expedient work-around if the "right way" is not easy.
- **Trusted User** - Generally trusted to handle sensitive information. May need to read and modify high sensitivity data at the same time as reading low sensitivity data.
- **Angry User** - Looking for ways to harm the enterprise.Not motivated to either expend a lot of energy to achieve damage, or to take risks that would result in getting caught.
- **Aggressive Incompetent User** - Not authorized to handle sensitive data, and generally will not violate a clear policy The biggest problem with this user is ignorance.
- **Vandal** - Motivated by boredom, desire for attention and/or just plain technical curiosity. Not motivated to expend significant resources, but is technically capable.
- **Professional Attacker** - Motive largely driven by resource values. Often interested in clandestine attacks that cannot be traced back to the attacker's organization.

IA Concepts

CyberCIEGE features a context-sensitive encyclopedia that allows the player to instantly call up relevant information regarding game play. Many of the concepts taught in CyberCIEGE have brief animated movies that help illustrate illusive concepts.



Success

During the game, the player's success is reflected in terms of how well the enterprise is doing (e.g., using a metric of dollars.) The player can query the "thoughts" of individual virtual users to view the user's level of happiness and current complaints and desires, such as: "I sure would like more convenient Internet access." After game play has completed, the player experiences a debriefing in which the player choices are critiqued by the system. To facilitate education and training, scenarios can be narrowly constructed to focus on specific topics. Lessons that should be learned in earlier scenarios can be incorporated into subsequent scenarios to gauge the player's ability to apply lessons learned to new situations.

Scenarios

Users of CyberCIEGE are encouraged to develop their own game scenarios and group them into larger game campaigns. CISR provides the tools necessary for CyberCIEGE users to create endless scenarios variations.

The Scenario Development Tool (SDT) automates the syntax of the CyberCIEGE scenario definition language through the use of several reusable libraries within a graphic user interface (GUI) and easy-to-use pull down menus.

The SDT is a great way for IA teachers to use CyberCIEGE to focus student attention on specific IA concepts.

Development

Development of CyberCIEGE was sponsored by the US Navy, the Naval Education and Training Command, the Office of Naval Research, and the Office of the Secretary of Defense. Numerous NPS students have participated in tool and scenario development.

Information

For more information regarding CyberCIEGE, visit our website at http://cisr.nps.navy.mil/cyberciege or contact:

Computer Science Department
Naval Postgraduate School
833 Dyer Road
Monterey, CA 93943
cyberciege@nps.edu

CISR The Center for Information Systems Security Studies and Research

http://cisr.nps.navy.mil/cyberciege/

NPS PRAESTANTIA PER SCIENTIAM 1909

NAVAL POSTGRADUATE SCHOOL

CyberCIEGE software was created by United States Government employees at The Center for Information Systems Security Studies and Research (CISR) at the Naval Postgraduate School (NPS) and Rivermind, Inc. CyberCIEGE contains government work created by NPS employees and therefore those portions of CyberCIEGE are in the public domain and are not subject to copyright. All remaining work within CyberCIEGE is copyrighted by Rivermind and its use is subject to the copyright protection afforded to Rivermind.

CyberCIEGE

Can you keep the network alive?

http://cisr.nps.navy.mil/cyberciege/

CISR The Center for Information Systems Security Studies and Research